welivesecurity

News, views, and insight from the ESET security community

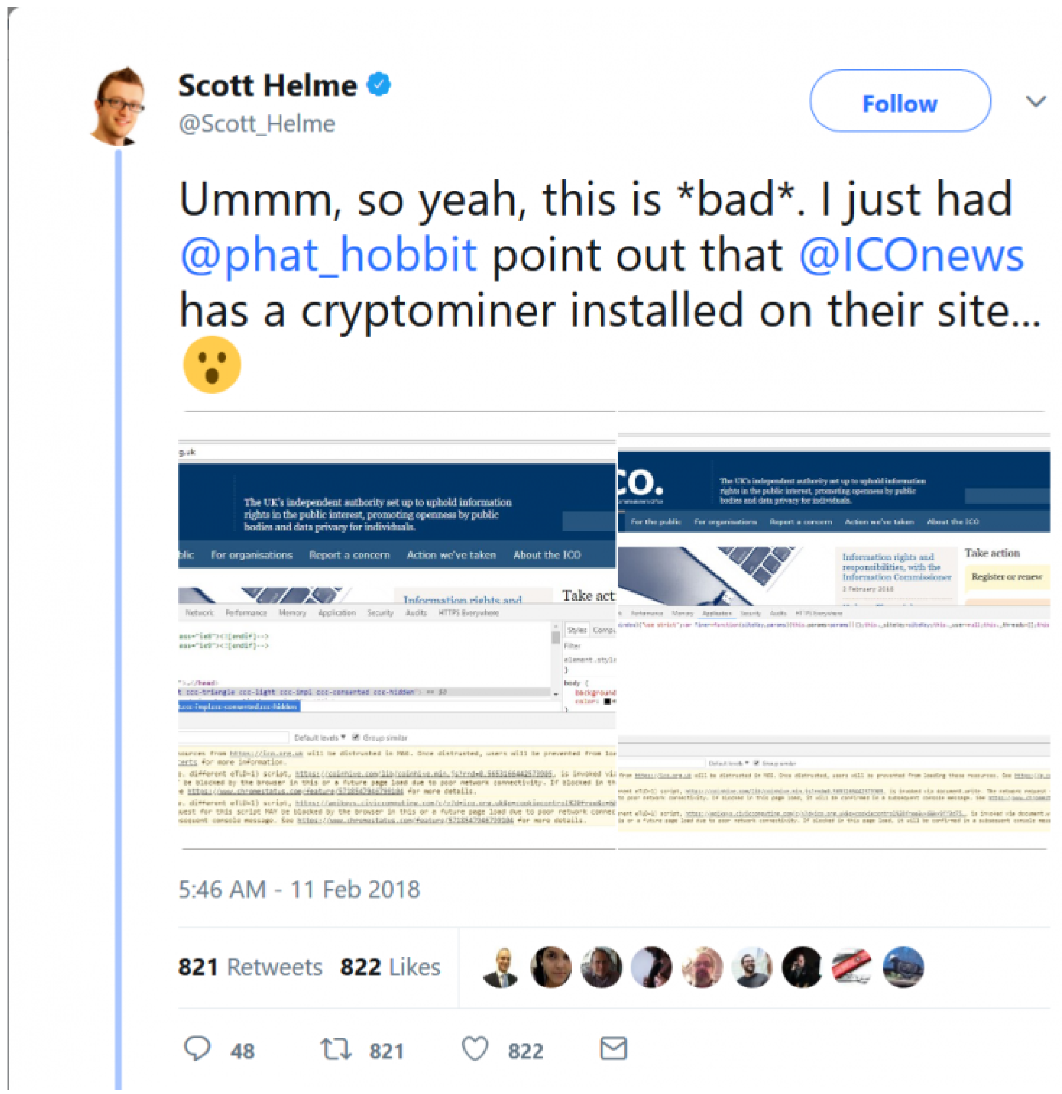
Type your keyword... Search

US and UK government websites hijacked to mine cryptocurrency on visitors' machines

BY TOMÁŠ FOLTÝN POSTED 12 FEB 2018 - 03:49PM

Over 4,200 websites worldwide, including many in the public sector in the United States, the United Kingdom and Australia, inadvertently became part of a scheme on Sunday in which attackers generated profits by forcing visitors' computers to surreptitiously mine a digital currency called Monero.

The latest major flare-up in covert cryptocurrency mining, a practice also known as cryptojacking, generated headlines after security researcher **Scott Helme** sounded the alarm on the hack on Sunday. He was alerted to the issue by another security professional, **Ian Thornton-Trump**, who had received a warning from his security software when visiting the website of the Information Commissioner's Office (ICO), the UK's data protection watchdog.



Scott Helme
@Scott_Helme

Ummm, so yeah, this is *bad*. I just had @phat_hobbit point out that @ICOnews has a cryptominer installed on their site... 😮

5:46 AM - 11 Feb 2018

821 Retweets 822 Likes

Follow
48
821
822
The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
For organisations
Report a concern
Action we've taken
About the ICO
Take action

Scott Helme tweeting about the ICO website compromise.
Image source: *Twitter*

The US courts' portal (uscourts.gov), various websites belonging to the UK's National Health System (NHS) services and many others made it to the **list** of 4,275 targets, many of them high-profile. They all load a plugin that had been maliciously tainted to add a stealthy cryptocurrency mining script known as CoinHive.

CoinHive inserted itself into the thousands of websites via Browsealoud, a third-party browser plugin that converts website text to speech for visually impaired visitors and for those with dyslexia or low literacy. If undetected by a user's security solution or content- or ad-blocker, the script ran in the background unbeknown to the user until the webpage was closed.

"If you want to load a crypto miner on 1,000+ websites you don't attack 1,000+ websites, you attack the 1 website that they all load content from," Helme said on his website.

“This type of attack isn’t new – but this is the biggest I’ve seen. A single company being hacked has meant thousands of sites impacted across the UK, Ireland and the United States,” Helme was quoted as **saying** for Sky News.

The plugin’s maker, Texthelp, **confirmed** that their product had been compromised at 11.14 am GMT on Sunday and had remained active for four hours.

“Texthelp has in place continuous automated security tests for Browsealoud, and these detected the modified file and as a result the product was taken offline. This removed Browsealoud from all our customer sites immediately, addressing the security risk without our customers having to take any action,” the company’s, CTO and Data Security Officer, Martin McKay said. He gave assurances that no customer data had been accessed or lost, nor that any data redirection had taken place.

A number of the affected websites, including that of the ICO, were also offline for hours in the aftermath of the attack.

The UK’s National Cyber Security Centre (NCSC) **said** that its experts are “examining data involving incidents of malware being used to illegally mine cryptocurrency”.

“The affected service has been taken offline, largely mitigating the issue. Government websites continue to operate securely. “At this stage there is nothing to suggest that members of the public are at risk,” reads the statement.

CoinHive has been detected on **thousands of websites** as well as in browser extensions and plugins since it was rolled out last September. While it was touted as a legitimate way for website owners to generate revenue using a method other than adverts, CoinHive has been co-opted by ne’er-do-wells looking to make a quick buck. The prevalence of the practice picked up extra steam as bitcoin and other **virtual currencies** soared in price.

Malicious **cryptocurrency miners** are also known to target **unpatched Windows webservers** and mobile devices.

Follow us